What is claimed is:

1. A method for initializing a series of electronic transactions, comprising the steps of:
   a. receiving an initialization request message that atomically binds
      i. authorization data, and
      ii. a blinded unvalidated certificate to be validated;
   b. determining if the authorization data is valid;
   c. if the authorization data is valid, then validating the blinded unvalidated certificate to obtain a blinded validated certificate; and
   d. sending an initialization response message to a registrant that includes the blinded validated certificate atomically bound to the initialization request message received in step a.

2. The method of claim 1, further comprising the step of receiving a registration acknowledgment message from a registrant acknowledging that the registrant has received the initialization response message.

3. The method of claim 1, wherein the initialization request message includes a nonce, a session key and a blinding factor applied to the nonce, and further comprising the step of storing the initialization request message and the initialization response message in a recovery database.

4. A method for recovering from an interruption in initializing an electronic transaction, comprising the steps of:

a. receiving a first initialization request message from a registrant that includes a nonce, a session key, and a blinding factor applied to the nonce, and that atomically binds

i. authorization data, and

ii. a blinded unvalidated certificate to be validated;

b. storing the initialization request message in a recovery database;

c. determining if the authorization data is valid;

d. if the authorization data is valid, then validating the blinded unvalidated certificate to obtain a blinded validated certificate;

e. sending a first initialization response message to a registrant that includes the blinded validated certificate atomically bound to the initialization request message received in step a;

f. storing the first initialization response message in a recovery database;

g. receiving a second initialization request message;

h. determining if the second initialization request message has the same nonce, session key, and blinding factor applied to the nonce as the

first initialization request message stored in the recovery database; and

i. if the second initialization request message has the same nonce, session key, and blinding factor applied to the nonce as the first initialization request message, then

1. retrieving the first initialization response message from the recovery database; and

2. sending the first initialization response message to the registrant.

5. A method for performing an electronic transaction, comprising the steps of:

a. receiving a transaction request message that atomically binds

i. an unblinded certificate, and

ii. a blinded unvalidated certificate to be validated;

b. determining if the unblinded certificate is valid; and

c. if the unblinded certificate is valid, then performing a transaction response that includes:

i. validating the blinded unvalidated certificate to obtain a validated blinded certificate, and

ii. sending the validated blinded certificate atomically bound to the transaction request message to a

transaction response recipient in a transaction response message.

6. The method of claim 5, wherein the transaction response further includes making available a product to a party.

7. The method of claim 5, wherein the transaction response further includes obtaining payment for a product.

8. The method of claim 5, further comprising the step of receiving a transaction acknowledgment message from a registrant acknowledging that the transaction response recipient has received the transaction response message.

9. The method of claim 5, further comprising the step of storing the transaction request message and the transaction response message in a recovery database.

10. A method for recovering from an interruption in an electronic transaction, comprising the steps of:

a. receiving a first transaction request message that includes a session key, a nonce and a blinding factor applied to the nonce, and that atomically binds

i. an unblinded certificate, and

ii. a blinded unvalidated certificate to be validated;

b. storing the first transaction request message in a recovery database;

c. determining if the unblinded certificate is valid; and

d. if the unblinded certificate is valid, then performing a transaction response that includes

i. validating the blinded unvalidated certificate to obtain a validated blinded certificate,

ii. sending the validated blinded certificate atomically bound to the transaction request message to a transaction response recipient in a first transaction response message, and

iii. storing the first transaction response message in a recovery database;

e. receiving a second transaction request message that includes a session key, a nonce and a blinding factor applied to the nonce, and that atomically binds

i. an unblinded certificate, and

ii. a blinded unvalidated certificate to be validated;

f. determining if the second transaction request message has the same nonce, session key, and blinding factor applied to the nonce as the first transaction request message stored in the recovery database; and

g. if the second transaction request message has the same nonce, session key, and blinding factor

applied to the nonce as the first transaction request message, then

i. retrieving the first transaction response message from the recovery database, and

ii. sending the first transaction response message to the transaction response recipient.

11. A method for auditing an electronic transaction, comprising the steps of:

a. receiving a transaction request message that atomically binds

i. an unblinded certificate,

ii. a blinded unvalidated certificate to be validated, and

iii. blinded audit data;

b. sending an audit request message atomically bound to the transaction request message to an audit recipient;

c. receiving an audit response message atomically bound to the audit transaction message, wherein the audit response message includes audit response data;

d. determining if the blinded audit data is valid using the audit response data.

12. The method of claim 11, wherein the audit response data is determined to be valid if

i. the audit response data corresponds to the blinded audit data received in the transaction request message, and

ii. the audit response data is legitimate.

13. An apparatus for initializing a series of electronic transactions, comprising:

a. a processor; and

b. a memory that stores instructions adapted to be executed by said processor to,

i. receive an initialization request message that atomically binds authorization data and a blinded unvalidated certificate to be validated;

ii. determine if the authorization data is valid;

iii. if the authorization data is valid, then to validate the blinded unvalidated certificate to obtain a blinded validated certificate; and

iv. send an initialization response message to a registrant that includes the blinded validated certificate atomically bound to the initialization request message,

said memory coupled to said processor.

14. The apparatus of claim 13, further comprising a port adapted to be coupled to a network, said port coupled to said memory and said processor.

15. An apparatus for performing an electronic transaction, comprising:

a. a processor; and

b. a memory that stores instructions adapted to be executed by a processor to

i. receive a transaction request message that atomically binds an unblinded certificate and a blinded unvalidated certificate to be validated;

ii. determine if the unblinded certificate is valid; and

iii. if the unblinded certificate is valid, then to perform a transaction response that validates the blinded unvalidated certificate to obtain a validated blinded certificate, and sends the validated blinded certificate atomically bound to the transaction request message to a transaction response recipient in a transaction response message,

said memory coupled to said processor.

16. The apparatus of claim 15, further comprising a port adapted to be coupled to a network, said port coupled to said memory and said processor.

17. An apparatus for auditing an electronic transaction, comprising:

a. a processor; and

b. a memory that stores instructions adapted to be executed by said processor to

i. receive a transaction request message that atomically binds an unblinded certificate and a blinded unvalidated certificate to be validated and blinded audit data;

ii. send an audit request message atomically bound to the transaction request message to an audit recipient;

iii. receive an audit response message atomically bound to the audit transaction message, where the audit response message includes audit response data; and

iv. determine if the blinded audit data is valid using the audit response data,

said memory coupled to said processor.

18. The apparatus of claim 17, further comprising a port adapted to be coupled to a network, said port coupled to said processor and said memory.

19. An apparatus for recovering from an interruption in an electronic transaction, comprising:

a. a processor; and

b. a memory that stores instructions adapted to be executed by said processor to

i. receive a first transaction request message that includes a session key, a nonce and a blinding factor applied to the nonce, and that atomically binds an unblinded

certificate and a blinded unvalidated certificate to be validated;

ii. store the first transaction request message in a recovery database;

iii. determine if the unblinded certificate is valid;

iv.. if the unblinded certificate is valid, then performing a transaction response that validates the blinded unvalidated certificate to obtain a validated blinded certificate, sends the validated blinded certificate atomically bound to the transaction request message to a transaction response recipient in a first transaction response message, and stores the first transaction response message in a recovery database;

v. receive a second transaction request message that includes a session key, a nonce and a blinding factor applied to the nonce, and that atomically binds an unblinded certificate and a blinded unvalidated certificate to be validated;

vi. determine if the second transaction request message has the same nonce, session key, and blinding factor applied to the nonce as the first transaction request message stored in the recovery database;

vii. if the second transaction request message has the same nonce, session key, and

blinding factor applied to the nonce as the first transaction request message, then to retrieve the first transaction response message from the recovery database and send the first transaction response message to the transaction response recipient,

said memory coupled to said processor.

20. The apparatus of claim 19, further comprising a port adapted to be coupled to a network, said port coupled to said processor and said memory.

21. A medium that stores instructions adapted to be executed by a processor to perform the steps of:

a. receiving an initialization request message that atomically binds
   i. authorization data, and
   ii. a blinded unvalidated certificate to be validated;
b. determining if the authorization data is valid;
c. if the authorization data is valid, then validating the blinded unvalidated certificate to obtain a blinded validated certificate; and
d. sending an initialization response message to a registrant that includes the blinded validated certificate atomically bound to the initialization request message received in step a.

22. A medium that stores instructions adapted to be executed by a processor to perform the steps of:

a. receiving a transaction request message that atomically binds

i. an unblinded certificate, and

ii. a blinded unvalidated certificate to be validated;

b. determining if the unblinded certificate is valid; and

c. if the unblinded certificate is valid, then performing a transaction response that includes

i. validating the blinded unvalidated certificate to obtain a validated blinded certificate, and

ii. sending the validated blinded certificate atomically bound to the transaction request message to a transaction response recipient in a transaction response message.

23. A medium that stores instructions adapted to be executed by a processor to perform the steps of:

a. receiving a transaction request message that atomically binds

i. an unblinded certificate,

ii. a blinded unvalidated certificate to be validated, and

iii. blinded audit data;

b. sending an audit request message atomically bound to the transaction request message to an audit recipient;

c. receiving an audit response message atomically bound to the audit transaction message, wherein the audit response message includes audit response data;

d. determining if the blinded audit data is valid using the audit response data.

24. A system for performing an electronic transaction, comprising:

a. means for receiving a transaction request message that atomically binds

i. an unblinded certificate, and

ii. a blinded unvalidated certificate to be validated;

b. means for determining if the unblinded certificate is valid; and

c. means for validating the blinded unvalidated certificate to obtain a validated blinded certificate; and

d. means for sending the validated blinded certificate atomically bound to the transaction request message to a transaction response recipient in a transaction response message.

25. The system of claim 24, further comprising means for auditing an electronic transaction.

26. The system of claim 24, further comprising means for initializing a series of electronic transactions.

27. The system of claim 24, further comprising means for recovering from an interruption in an electronic transaction.